Hypershift

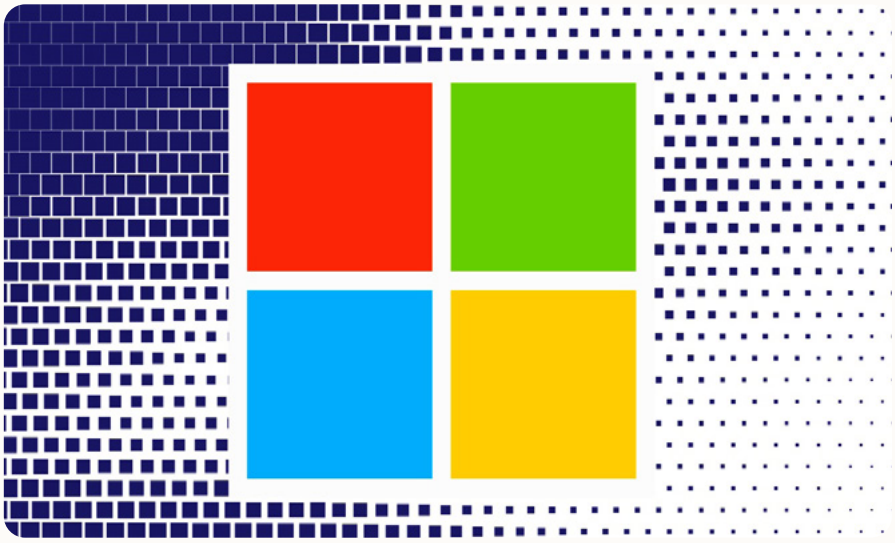
HYPERSHIFT.COM

CHECKLIST

MICROSOFT'S SECURE BOOT CERTIFICATE READINESS CHECKLIST

Plan & Deploy Your Secure Boot Certificate Expiration Plan With Some Help From Hypershift

WHY THIS CHECKLIST EXISTS



The June 2026 Secure Boot certificate expiration is an important readiness milestone for organizations running Microsoft environments. While Microsoft is providing updated Secure Boot certificates through supported update channels, many IT teams are discovering that successful remediation involves far more than standard Windows patching.

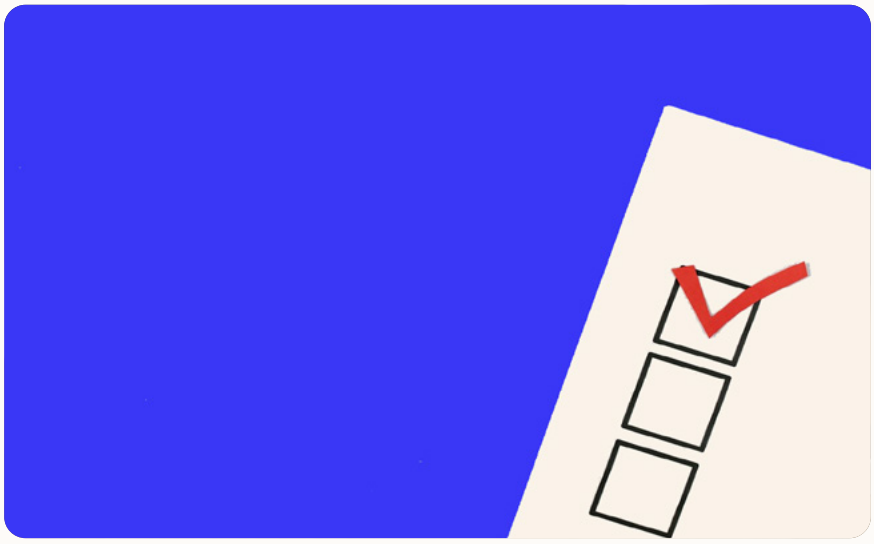
Unmanaged or aging devices can all impact whether systems successfully transition to the newer 2023 Secure Boot trust chain before the older 2011 certificates expire.

Firmware compatibility, reboot orchestration, BitLocker recovery behavior, server and virtual machine exposure, recovery media, and unmanaged or aging devices can all impact whether systems successfully transition to the newer 2023 Secure Boot trust chain before the older 2011 certificates expire.

This guide was created to help IT leaders and infrastructure teams assess operational readiness, identify hidden exposure, and build a practical remediation strategy before deadlines create unnecessary disruption.

Inside, you'll find a detailed readiness checklist, deployment guidance, common gaps organizations overlook, and a Secure Boot Readiness Scorecard to help evaluate your current posture across endpoints, servers, VMs, and recovery workflows.

SECURE BOOT PREPARATION CHECKLIST



1. Inventory Your Complete Device Estate

Before any remediation begins, build a clear view of every system that may depend on the Secure Boot certificate chain. Confirm inventory coverage for:

- ☐ **Windows 10 and Windows 11 endpoints**
- ☐ **Windows Server systems**
- ☐ **Virtual machines**
- ☐ **Remote and hybrid workforce devices**
- ☐ **Shared workstations and kiosk devices**
- ☐ **Legacy PCs still in production**
- ☐ **Lab, clinical, branch, warehouse, and manufacturing end-points**
- ☐ **Devices outside standard Intune, Autopatch, SCCM, RMM, or GPO management**
- ☐ **Recently acquired devices from mergers, acquisitions, or departmental purchases**
- ☐ **Dual-boot systems, especially Linux environments such as Red Hat Enterprise Linux or Fedora**
- ☐ **Devices with custom bootloaders, specialized imaging, or nonstandard firmware settings**
- ☐ **Systems with Secure Boot disabled, partially configured, or inconsistently reported**

Gaps IT Teams Often Miss

Many organizations already have inventory, but not the kind of inventory this event requires. A standard asset report may show device name, user, OS version, and serial number, but miss the details that actually matter for Secure Boot readiness.

Your inventory should capture:

- ☐ **Secure Boot enabled or disabled status**
- ☐ **Current Secure Boot certificate state, including whether the device is booting from the 2011 or 2023 trust chain**
- ☐ **Firmware vendor and version**
- ☐ **Device model and generation**
- ☐ **TPM status**
- ☐ **BitLocker status**
- ☐ **Windows update compliance**
- ☐ **BIOS or UEFI mode**
- ☐ **Whether the device is domain-joined, Entra-joined, hybrid-joined, or unmanaged**
- ☐ **Whether the device is receiving firmware updates through OEM tools, Windows Update, Intune, or manual processes**

Common Mistakes

The most common mistake is treating “managed by Intune” as equivalent to “ready,” or treating “policy applied” as equivalent to “device protected.” Neither is true for this transition. Intune coverage is helpful, but it does not guarantee firmware readiness, certificate presence, BitLocker behavior, or OEM compatibility across every model.

IT Leader Question

Can your team produce a list today of devices that are running older Secure Boot trust anchors, have outdated firmware, or are unmanaged? If the answer is **no**, that is the starting point.

2. Verify the New 2023 Certificates Are Present ✅

The goal is to ensure devices have the updated Secure Boot trust chain before the older 2011 certificates expire.

Microsoft identifies the expiring certificates as including the Microsoft Corporation KEK CA 2011, Microsoft Corporation UEFI CA 2011, and Microsoft Windows Production PCA 2011, with updated 2023 certificates replacing them across the KEK and DB trust stores.

You'll need to validate whether applicable devices have the updated certificates, including:

- ☐ **Microsoft Corporation KEK 2K CA 2023**
- ☐ **Microsoft UEFI CA 2023**
- ☐ **Microsoft Option ROM UEFI CA 2023**
- ☐ **Windows UEFI CA 2023**

Use available Microsoft guidance and tools to inspect Secure Boot state through approved methods such as PowerShell, event logs, Windows Update reporting, Windows Autopatch reporting, or enterprise management platforms.

Gaps IT Teams Often Miss

Certificate presence is not always binary from an operational perspective. A device can sit at Stage 4, where the 2023 certificate is already written to the UEFI database, but the machine is still booting from the old 2011 chain. It will sit there for weeks until a reboot happens. From the Intune dashboard, the device looks like it is making progress. In reality, it is not yet protected.

Pay special attention to:

- ☐ **Devices that have received the certificate update but have not rebooted**
- ☐ **Devices stuck in Stage 4 because users defer restarts indefinitely**
- ☐ **Devices on Hotpatch, where reboot cycles are rare by design**
- ☐ **Devices throwing Error 65000 (**Windows Pro and Subscription-Activated Enterprise devices, a known Microsoft licensing issue partially patched in January 2026**)**
- ☐ **Devices with pending firmware updates**
- ☐ **Devices that are powered off or rarely connected**
- ☐ **Devices with interrupted update histories**
- ☐ **VMs created from older templates**
- ☐ **Server workloads with conservative patch windows**
- ☐ **Systems managed by separate business units or acquired IT teams**

Common Mistake

Trusting the compliance dashboard at face value. A green or yellow dashboard often means the certificate landed in the database, not that the device is actually booting from the new trust chain. Those are two different states with two different risk profiles.

IT Leader Question

Do you have proof that the new Secure Boot certificates are not only present, but actively in use across your endpoint, server, and VM estate, or only an assumption that updates have been applied?

3. Ensure Windows Updates Are Current and Not Blocked

Microsoft is rolling updated Secure Boot certificates through regular Windows update channels for supported endpoint devices, and organizations can also manage the update process using their preferred tools.

For many IT environments, the largest obstacle will not be the update itself. It will be the policies, exceptions, deferrals, and operational habits that prevent the update from reaching every device.

Review update controls across:

- ☐ **Microsoft Intune update rings**
- ☐ **Windows Autopatch policies**
- ☐ **Windows Update for Business settings**
- ☐ **Group Policy update deferrals**
- ☐ **SCCM or Microsoft Configuration Manager deployments**
- ☐ **RMM patching tools**
- ☐ **WSUS approvals**
- ☐ **Maintenance windows**
- ☐ **Quality update deferrals**
- ☐ **Feature update holds**
- ☐ **Driver and firmware update exclusions**
- ☐ **Devices paused because of previous patching incidents**

Gaps IT Teams Often Miss

Look for good intentions that create hidden risk:

- ☐ **Update rings that defer cumulative updates too long**
- ☐ **Firmware updates intentionally excluded from Windows Update**
- ☐ **Pilot rings that never graduate to broad deployment**
- ☐ **Devices stuck in exception groups**
- ☐ **Servers patched under different governance than endpoints**
- ☐ **Remote laptops that have not connected long enough to complete the update cycle**
- ☐ **Reboot policies that allow users to defer restarts indefinitely**
- ☐ **Security tools that interfere with update completion**
- ☐ **Legacy VDI or golden image templates that are not refreshed**

Common Mistake

A dashboard showing compliant may only mean compliant with the organization's current update policy, not necessarily compliant with the Secure Boot certificate transition.

IT Leader Question

Are your update policies accelerating Secure Boot readiness, or quietly delaying it?

4. Staged Ring Approach For OEM Firmware Updates

This is likely the most underestimated part of the project.

Secure Boot sits at the intersection of Windows, firmware, certificates, hardware drivers, bootloaders, and OEM implementation.

Microsoft has emphasized ecosystem collaboration with device manufacturers and firmware partners as part of this Secure Boot refresh.

That means IT teams should treat this like a controlled infrastructure change, not a routine endpoint patch.

Build a firmware readiness plan that includes:

- ☐ **Hardware model inventory**
- ☐ **Firmware version inventory**
- ☐ **OEM support status**
- ☐ **BIOS or UEFI update availability**
- ☐ **Known compatibility issues by model**
- ☐ **Pilot groups by device family**
- ☐ **Test devices for each major hardware configuration**
- ☐ **Reboot and rollback planning**
- ☐ **Firmware update deployment method**
- ☐ **Helpdesk escalation procedures**
- ☐ **Business unit communication**
- ☐ **Change window scheduling**
- ☐ **Executive visibility for high-risk device groups**
- ☐ **Windows UEFI CA 2023**

Recommended Ring Structure

Use a staged rollout model:

Ring 0: IT Lab Validation. Test representative devices across major OEMs, models, firmware versions, and use cases.

Ring 1: IT Department and Low-Risk Pilot Users. Deploy to technically capable users who can quickly report issues.

Ring 2: Standard Business Users. Expand to a controlled group across departments, locations, and device types.

Ring 3: High-Volume Production Rollout. Deploy broadly after telemetry, helpdesk scripts, and rollback processes are validated.

Ring 4: Sensitive and Specialized Systems. Handle executives, clinical systems, financial operations, manufacturing devices, shared workstations, servers, and regulated workloads with dedicated planning.

Gaps IT Teams Often Miss

Firmware programs often fail because the team treats all laptops as interchangeable. They are not. Risk varies by:

- ☐ **OEM**
- ☐ **Model**
- ☐ **BIOS version**
- ☐ **Docking station configuration**
- ☐ **Option ROMs**
- ☐ **Third-party boot components**
- ☐ **Encryption state**
- ☐ **Peripheral dependencies**
- ☐ **Region-specific hardware procurement**
- ☐ **Age of device**
- ☐ **Whether the system has ever received firmware updates**

Common Mistake

Do not start with a broad firmware deployment across the whole estate. A single model-specific issue can create a wave of tickets, executive disruption, and rollback complexity.

IT Leader Question

Have you validated Secure Boot certificate updates on the actual hardware combinations your business runs every day?

5. Manage BitLocker Before It Manages Your Helpdesk

Secure Boot changes can affect BitLocker behavior. In some configurations, updates to Secure Boot variables may trigger BitLocker recovery. That does not mean the update is wrong, but it does mean the rollout needs operational discipline.

Before deployment, confirm:

- ☐ **BitLocker recovery keys are escrowed and accessible**
- ☐ **Recovery keys are stored in Entra ID, Active Directory, or the approved enterprise repository**
- ☐ **Helpdesk has a documented recovery process**
- ☐ **Users know what to do if prompted**
- ☐ **BitLocker suspension policy is defined**
- ☐ **Suspension duration is appropriate and controlled**
- ☐ **Security approval exists for any temporary suspension**
- ☐ **Devices resume protection after updates**
- ☐ **Exceptions are tracked and closed**
- ☐ **VIP and executive devices receive special handling**

Common Mistake

Suspending BitLocker without a clear resume policy creates a new security gap while trying to close an old one.

IT Leader Question

If 50 users received a BitLocker recovery prompt tomorrow morning, could your team recover them quickly, securely, and consistently?

Gaps IT Teams Often Miss

The biggest BitLocker risk is not the recovery event itself. It is the operational scramble when the helpdesk cannot quickly retrieve the recovery key or users do not know whether the prompt is legitimate.

Before rollout, verify:

- ☐ **Recovery key escrow health**
- ☐ **Helpdesk access permissions**
- ☐ **MFA requirements for support technicians**
- ☐ **After-hours support coverage**
- ☐ **Remote worker recovery process**
- ☐ **Communication templates**
- ☐ **Documentation for non-technical users**
- ☐ **Process for devices assigned to terminated employees**
- ☐ **Process for stale or duplicate device records**

Common Mistake

Suspending BitLocker without a clear resume policy creates a new security gap while trying to close an old one.

IT Leader Question

If 50 users received a BitLocker recovery prompt tomorrow morning, could your team recover them quickly, securely, and consistently?

Additional Readiness Areas Most Checklists Miss

6. Assess Windows Server and Virtual Machine Exposure

Servers are not a smaller version of the endpoint problem. They are a separate problem.

Here is the part most teams miss: Windows Server does not receive the 2023 Secure Boot certificates automatically through Windows Update the way Windows 11 endpoints do. For servers, the certificate update is a manual deployment exercise. Same story for Generation 2 Hyper-V virtual machines. They need the update pushed in, it does not arrive on its own.

If you have 50 servers, that is 50 manual remediation jobs that nobody has started yet.

Review:

- ☐ **Physical Windows servers**
- ☐ **Hyper-V hosts (the host firmware itself)**
- ☐ **Generation 2 Hyper-V virtual machines**
- ☐ **VMware-based Windows workloads (firmware update happens on the hypervisor side)**
- ☐ **Azure VMs, especially Trusted Launch and Confidential VMs**
- ☐ **Disaster recovery replicas**
- ☐ **Backup validation environments**
- ☐ **Server templates**
- ☐ **Golden images**
- ☐ **Domain controllers**
- ☐ **Remote Desktop Session Hosts**
- ☐ **Legacy application servers**
- ☐ **File, print, and utility servers**
- ☐ **Systems with infrequent reboot cycles**

Important Scope Note

Generation 1 Hyper-V VMs do not use UEFI firmware, so they are not affected by this transition. Do not waste cycles remediating them.

Common Mistake

Assuming that because servers receive monthly Windows updates, they are also receiving the Secure Boot certificate updates. They are not. This is a manual project for the server fleet, and it has the same June and October 2026 deadlines as everything else.

IT Leader Question

Who owns the Secure Boot remediation plan for your server estate, and is it on the same timeline as your endpoint plan?

7. Refresh Golden Images, Autopilot Profiles, Build Processes, and Recovery Media

Even if production devices are remediated, outdated provisioning and recovery artifacts can reintroduce the same risk months later.

Recovery media is the sleeper issue here. A WinPE stick, a recovery USB, or an install image created before the 2023 certificates were adopted can fail to boot on firmware that has moved to the new trust chain. You fix the fleet today, six months from now your helpdesk pulls out an old USB to reimage a laptop, and it does not boot. The remediation worked. The recovery process is broken.

Update and validate:

- ☐ **Windows Autopilot deployment profiles**
- ☐ **Golden images**
- ☐ **Task sequences**
- ☐ **VM templates (Generation 2 only)**
- ☐ **WinPE recovery media**
- ☐ **Bootable USB recovery sticks**
- ☐ **Installation media used by helpdesk and field technicians**
- ☐ **Break-glass admin workstations**
- ☐ **Loaner device images**
- ☐ **New hire provisioning workflows**
- ☐ **OEM factory image assumptions**
- ☐ **Driver and firmware packages**

Common Mistake

Fixing the current fleet while continuing to deploy new devices and recover broken ones from outdated images and media. This creates a slow, invisible regression. Every new build or recovery event reintroduces the old trust chain into your environment.

IT Leader Question

When was the last time your team rebuilt the WinPE stick that lives in the helpdesk drawer?

8. Identify Unsupported or Near-End-of-Life Hardware

This event is a forcing function for hardware lifecycle decisions.

Some devices may be technically possible to remediate, but not operationally wise to keep. Older devices with unreliable firmware support, inconsistent update behavior, or poor visibility may create more risk than value.

Flag devices that are:

- ☐ **Out of warranty**
- ☐ **No longer supported by the OEM**
- ☐ **Unable to receive firmware updates**
- ☐ **Running unsupported Windows versions**
- ☐ **Frequently offline**
- ☐ **Assigned to critical users**
- ☐ **Used in regulated workflows**
- ☐ **Missing TPM or Secure Boot readiness**
- ☐ **Experiencing repeated update failures**
- ☐ **Better suited for replacement than remediation**

Common Mistake

Trying to save every aging device can consume more labor than replacing the highest-risk group.

IT Leader Question

Which devices should be remediated, and which should become part of a controlled refresh plan?

9. Validate Compliance and Audit Requirements

For finance and healthcare organizations, this is more than an IT maintenance task. It intersects with security governance, audit readiness, cyber insurance expectations, and regulatory posture.

Document:

- ☐ **Inventory scope**
- ☐ **Risk assessment**
- ☐ **Remediation plan**
- ☐ **Exception handling**
- ☐ **Testing results**
- ☐ **Deployment rings**
- ☐ **Change approvals**
- ☐ **BitLocker procedures**
- ☐ **Firmware update plan**
- ☐ **Completion evidence**
- ☐ **Deferred or unsupported systems**
- ☐ **Executive sign-off**

Common Mistake

Completing the technical work without preserving evidence leaves IT exposed during audits, incident reviews, or insurance assessments.

10. Prepare Communications Before the First Rollout

The technical project will go smoother if users, helpdesk, security, and leadership understand what is happening.

Prepare communications for:

- ☐ **Executive stakeholders**
- ☐ **Department leaders**
- ☐ **Helpdesk teams**
- ☐ **Security and compliance teams**
- ☐ **Remote employees**
- ☐ **VIP users**
- ☐ **Users with older hardware**
- ☐ **Users who may see BitLocker recovery prompts**
- ☐ **Teams affected by reboot windows**

11. Hotpatch Devices Need Special Handling

If your fleet uses Windows Hotpatch, you have a unique exposure. Hotpatching is designed to reduce reboot frequency. That is a feature for normal patching, but for the Secure Boot certificate transition it is a problem.

The 2023 certificate cannot finish activating without a reboot. On a Hotpatch device, that reboot may not happen for weeks. Meanwhile, the device shows up in dashboards as update applied while it is still booting from the 2011 chain.

For Hotpatch fleets, build a scheduled reboot orchestration plan that runs alongside the certificate rollout. Otherwise, the dashboard will keep telling you everything is fine while your real risk does not move.

IT Leader Question

Do you know which of your devices are on Hotpatch, and when each one last completed a full reboot?

The Secure Boot Readiness Scorecard

IT leaders can use this as a fast internal assessment

Readiness Area	Green	Yellow	Red
Device Inventory	COMPLETE ENDPOINT, SERVER, VM, FIRMWARE, AND SECURE BOOT VISIBILITY	INVENTORY EXISTS BUT LACKS FIRMWARE OR CERTIFICATE DETAIL	UNKNOWN, FRAGMENTED, OR SPREADSHEET-BASED
Certificate Validation	2023 CAS CONFIRMED ACROSS REPRESENTATIVE SYSTEMS	VALIDATION UNDERWAY BUT INCOMPLETE	ASSUMED COVERED BY UPDATES
Windows Updates	RINGS REVIEWED, CUMULATIVE UPDATES FLOWING, REBOOTS ENFORCED	SOME DEFERRALS OR EXCEPTION GROUPS REMAIN	UPDATES BLOCKED, DEFERRED, OR INCONSISTENT
Firmware	OEM MODEL-LEVEL PLAN IN PLACE	FIRMWARE PLAN EXISTS FOR SOME DEVICES	NO FIRMWARE STRATEGY
BitLocker	KEYS ESCROWED, PROCESS DOCUMENTED, HELPDESK TRAINED	PARTIAL ESCROW OR UNCLEAR SUSPENSION PROCESS	RECOVERY PROCESS UNTESTED
Servers & VMs	MANUAL DEPLOYMENT PLAN IN PLACE, GEN 2 VMS SCOPED	PARTIALLY ASSESSED	NOT INCLUDED
Golden Images & Recovery Media	UPDATED, VALIDATED, WINPE REFRESHED	PLANNED BUT NOT COMPLETE	NOT REVIEWED
Hotpatch Devices	REBOOT ORCHESTRATION IN PLACE FOR CERT ACTIVATION	AWARE OF ISSUE, NO PLAN	NOT IDENTIFIED
Unsupported Hardware	IDENTIFIED WITH REFRESH RECOMMENDATIONS	PARTIAL LIFECYCLE DATA	UNKNOWN EXPOSURE
Compliance Evidence	DOCUMENTED AND REPORTABLE	SOME EVIDENCE CAPTURED	NO AUDIT TRAIL
Comms	HELPDESK AND USERS BRIEFED	DRAFT COMMUNICATIONS EXIST	NO COMMUNICATION PLAN

Get a Free Secure Boot Risk Report

Delivered in 3 business days.

The report identifies:

- ✓ **Devices at risk**
- ✓ **Missing certificate indicators**
- ✓ **Stage 4 devices (certificate landed but not yet booting from the 2023 chain)**
- ✓ **Hotpatch devices that need reboot orchestration**
- ✓ **Firmware exposure**
- ✓ **BitLocker recovery risk**
- ✓ **Windows update policy blockers**
- ✓ **Unsupported or aging hardware**
- ✓ **Server, VM, and recovery media considerations**
- ✓ **Recommended remediation path**
- ✓ **Estimated effort by device population**
- ✓ **Priority actions before June 2026**

After the report, we provide remediation through a firm fixed price engagement.

Our Guarantee: We complete remediation within 14 days or your money back.

Remediation Packages

COMPANY SIZE	ESTIMATED REMEDIATION BLOCK
SMALL COMPANIES, 300 USERS OR LESS	10 HOURS
MEDIUM COMPANIES, 301 TO 1,000 USERS	20 HOURS
LARGE COMPANIES, 1,000+ USERS	60 HOURS

Ready to get ahead of the Secure Boot expiration? Our experts assess your exposure, identify remediation priorities, and provide a clear path to eliminate risk.

Click Here To Get Your Risk Report

ABOUT HYPERSHIFT

We're dedicated to championing businesses' digital evolution. Our team offers top-tier consulting on new and emerging technologies, encompassing enterprise infrastructure, cloud solutions, networking, security, and analytics.

Let us pave the way for your organization to keep moving forward. Our experts are well-versed in both traditional data centers and modern cloud environments. We guide businesses in seamlessly integrating these platforms, ensuring a tailored approach that aligns with their unique objectives.

While we specialize in mid-sized companies, we have partnered with companies of all sizes, including Fortune 100 giants. Our Hypershift managed service division is trusted by over 160 financial institutions. We take pride in being a part of CISA's critical security infrastructure initiative, which helps safeguard organizations.

Our team is our secret weapon. With 6 CCIE-certified engineers (some who've even earned it multiple times) and over 50 experienced consultants, we have the expertise to handle any size organization.

We can confidently manage even the most complex networks with efficiency and precision.

We don’t go it alone. With over 70 industry-leading partners, such as Cisco and Nutanix, we offer a comprehensive range of solutions and consulting services.

Let Hypershift be a trusted partner in pushing your organization forward with better technology.

Schedule a consultation

hello@hypershift.com